



AEROSPACE INFORMATION REPORT

AIR7209™

Issued

2022-10

Development Assurance Principles for Aerospace Vehicles and Systems

RATIONALE

This SAE Aerospace Information Report (AIR) provides a high-level set of principles for the development assurance of aerospace vehicles and systems, including emerging technologies. The principles are meant to address experience of applying ARP4754/ED-79 (at latest revision) across a variety of applications. This document is technically identical to ER-023. If further elaboration of specific technologies is determined to be required, additional AIRs/ERs may be created.

TABLE OF CONTENTS

1.	SCOPE.....	2
1.1	Purpose.....	2
1.2	Background.....	2
2.	References.....	2
2.1	Applicable Documents.....	2
2.1.1	SAE Publications.....	2
2.1.2	FAA Publications.....	3
2.2	Definitions.....	3
3.	DEVELOPMENT ASSURANCE PRINCIPLES.....	4
3.1	Overview.....	4
3.2	Define the Development Assurance Process.....	6
3.2.1	Identify Planned Activities.....	6
3.3	Perform Supporting Processes.....	6
3.3.1	Perform Process Assurance.....	6
3.3.2	Manage Product Configuration.....	7
3.3.3	Manage Development Errors.....	7
3.3.4	Manage Assumptions.....	7
3.4	Define the Product.....	8
3.4.1	Identify Product Functions.....	8
3.4.2	Define and Validate Requirements.....	8
3.4.3	Identify Functional Safety Effects.....	9
3.4.4	Analyze Proposed Architecture.....	9
3.5	Evaluate the Implementation.....	10
3.5.1	Verify Implementation.....	10
3.5.2	Assess Unintended Behaviors.....	10
3.5.3	Evaluate Implementation.....	10
4.	NOTES.....	11
4.1	Revision Indicator.....	11
Figure 1	Development assurance principles.....	5

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2022 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

For more information on this standard, visit
<https://www.sae.org/standards/content/AIR7209/>

1. SCOPE

1.1 Purpose

The purpose of this SAE Aerospace Information Report (AIR) is to provide a high-level set of principles to support aerospace projects required to use a formal development assurance process, such as ARP4754/ED-79 (at latest revision), to show regulatory compliance. Examples of projects where a formal development assurance process is needed are those that have significant functional interactions or whose products cannot be fully analyzed or tested. Development assurance techniques reduce the likelihood of undetected errors that could have safety impacts in the operation of the product. Design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for more complex systems.

This document does not mandate specific processes to meet each development assurance principle. These principles are written at a high level to allow flexibility so that users can develop and evaluate their own compliant development assurance processes. Users are responsible for presenting their development assurance approach to certification authorities and obtaining agreement. The framework in this document can assist with this coordination.

1.2 Background

The industry has commonly relied on ARP4754/ED-79 (at latest revision) for guidelines for development assurance processes. However, ARP4754/ED-79 (at latest revision) has presented several challenges:

- a. Some potentially effective development assurance methods are not adequately addressed by ARP4754/ED-79 (at latest revision) techniques (e.g., system level application of formal methods, model-based system engineering, systems theoretic process analysis).
- b. Novel technologies are not adequately addressed by ARP4754/ED-79 (at latest revision) techniques (e.g., neural networks, artificial intelligence, machine learning).
- c. Developers have had difficulty obtaining acceptance of existing company processes and practices that meet the intent of ARP4754/ED-79 (at latest revision).
- d. ARP4754/ED-79 (at latest revision) has been misinterpreted or misapplied, requiring activities that were intended as recommendations.

The development assurance principles in this document describe the fundamental principles from ARP4754/ED-79 (at latest revision). These principles provide a framework within which these challenges may be addressed. ARP4754/ED-79 (at latest revision) remains one means, but not the only means, of meeting these principles. Users are responsible for coordinating their development assurance approach with certification authorities.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

ARP4754/ED-79 Guidelines for Development of Civil Aircraft and Systems

2.1.2 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

AC 25.1309 System Design and Analysis

TAESdaT2-5241996 Task 2 - System Design and Analysis Harmonization and Technology Update

2.2 Definitions

ANALYSIS: A detailed examination based on decomposition into simple elements.

COMMON CAUSE: A single failure, error, or event that can produce undesirable effects on two or more systems, equipment, items, or functions.

DEVELOPMENT ASSURANCE: All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that development errors have been identified and corrected such that the system satisfies the applicable safety objectives. (Adapted from AC 25.1309)

DEVELOPMENT ERROR: A mistake in requirements determination, design, or implementation.

ERROR: An omitted or incorrect action by a manufacturer, operator, or maintenance person, or a mistake in requirements, design, or implementation. (Adapted from AC 25.1309.)

FAILURE: An occurrence that affects the operation of a product such that it can no longer function as intended. This includes both loss of function and malfunction. Note: Errors may cause failures, but are not considered to be failures. (Adapted from AC 25.1309.)

FAILURE CONDITION: A condition having an effect on the aerospace vehicle and/or its occupants, either direct or consequential, that is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events. The condition may have effects on third parties and critical infrastructure. (Adapted from AC 25.1309.)

FAILURE CONDITION CLASSIFICATION: A discrete scale allowing categorization of the severity of the effects of a failure condition. Classification levels are defined in the applicable regulation and advisory material. For example, AC 25.1309 draft ARSENAL (ARAC report TAESdaT2-5241996 includes AC/AMJ 25.1309 Draft ARSENAL revised System Design and Analysis) and AC 25.1309 define the following classifications: catastrophic, hazardous, major, minor, and no safety effect.

FUNCTION: Intended behavior of a product regardless of implementation.

HAZARD: A condition resulting from failures, external events, errors, or a combination thereof where safety is potentially affected.

PROCESS: A set of interrelated activities performed to produce a prescribed output or product.

PROCESS INDEPENDENCE: A practice that minimizes the likelihood of development errors by using separation of responsibilities that assures the accomplishment of objective evaluation by someone other than the performer of the activity, e.g., validation activities are not performed solely by the developer of the requirement(s) of a product.

PRODUCT: An aerospace vehicle or system (this is different from the regulatory Part 21 definition).

REQUIREMENT: A necessary physical and/or functional characteristic of a product that can be validated and against which an implementation can be verified.

SAFETY: The state in which risk is acceptable.

SAFETY OBJECTIVE: A qualitative and/or quantitative attribute necessary to achieve the required level of safety for the identified failure condition, depending on its classification.

SYSTEM: A defined combination of subsystems, equipment, or items that perform one or more specific functions.

UNINTENDED BEHAVIOR: Unexpected operation of a product in ways contrary to its intended functionality.

VALIDATION: The determination that the requirements for a product are correct and complete.

VERIFICATION: The evaluation of an implementation of requirements to determine that they have been met.

3. DEVELOPMENT ASSURANCE PRINCIPLES

3.1 Overview

The development assurance principles in this document are grouped into the following sections:

- a. **Define the development assurance process:** The principle in this section establishes the development assurance process to be used for the product's development. As described in Section [1](#), users of this document are responsible for presenting their development assurance approach to certification authorities and obtaining agreement.
- b. **Perform supporting processes:** The principles in this section are essential for effective development assurance and impact all principles in the other sections. These principles are met continuously or repetitively throughout the product's development.
- c. **Define the product:** The principles in this section are typically met prior to product implementation. They guide the identification and validation of what the product is expected to do and the analysis of the proposed product architecture.
- d. **Implement the product:** Implementation of the product is performed outside the scope of the processes described in this document.
- e. **Evaluate the implementation:** The principles in this section are typically met after product implementation. They guide verification that the implementation meets its corresponding requirements, does not exhibit undesirable or unsafe effects, and is safe for its intended use.

[Figure 1](#) provides an illustration of the development assurance principles during product development.

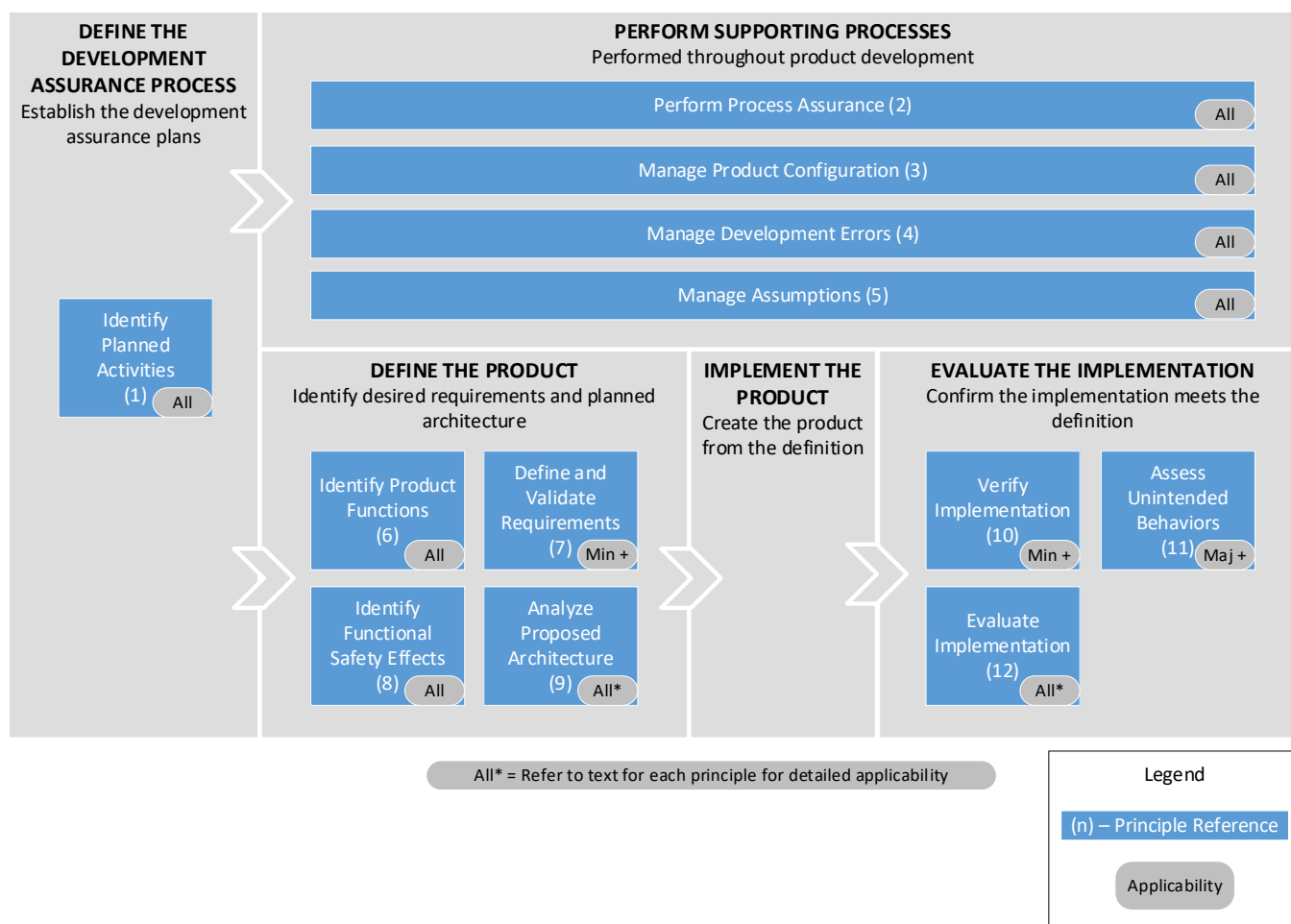


Figure 1 - Development assurance principles

These principles are shown here in a linear representation of their relationship, but some may be applied in practice in an iterative and concurrent manner.

An initial estimate of the failure condition classifications may be made as input to start the overall development assurance process. The failure condition classifications are then refined as the development assurance process is performed. Applicability in [Figure 1](#) indicates the lowest failure condition classification to which the principle would apply. The failure condition classifications used in this document are based upon AC 25.1309. If alternative failure condition classifications are used, the development assurance plan should provide definition and justification.

The following sections each begin by identifying a process principle in a small table. These tables include a reference number, the principle, and a statement of applicability (also annotated in each principle above). The text that follows each principle identifies the fundamental criteria for a process to meet the principle.

3.2 Define the Development Assurance Process

3.2.1 Identify Planned Activities

Ref	Principle	Applicability
1	The development assurance process ensures that planned activities for the product's development assurance are identified and recorded.	All failure condition classifications

A development assurance process that meets this principle:

- a. Identifies expected inputs for the development assurance process.
- b. Identifies data and deliverables produced.
- c. Defines interrelationships within and between processes, including feedback mechanisms and transition criteria.
- d. Defines roles and responsibilities of those involved, including planned process independence.
- e. Describes how each development assurance principle in this document is accomplished, including discussion of how the processes are modulated by failure condition classification.
- f. Identifies parts of the product, activities, or deliverables that are planned to be reused from a previous implementation and describes how these reused elements are evaluated for acceptability for the planned product.
- g. Defines how feedback from in-service data will be addressed throughout the lifecycle of the product.
- h. Describes how the data and deliverables will be summarized to show that all planned activities have been completed successfully.

3.3 Perform Supporting Processes

3.3.1 Perform Process Assurance

Ref	Principle	Applicability
2	The development assurance process ensures that activities are conducted according to the plan(s) and that process deviations are managed.	All failure condition classifications

A development assurance process that meets this principle:

- a. Confirms that development assurance process was conducted according to the plan(s) throughout development.
- b. Defines a process to identify and record process deviations.
- c. Defines a process to disposition process deviations, by either resolving the deviation or determining that the impacts of the deviation are acceptable.

3.3.2 Manage Product Configuration

Ref	Principle	Applicability
3	The development assurance process ensures that the data and deliverables are consistent and aligned with the product design.	All failure condition classifications

A development assurance process that meets this principle:

- a. Describes how product design and associated data and deliverables are identified.
- b. Describes how changes to the configuration definition are controlled and recorded.
- c. Describes how the effects of configuration changes will be evaluated for impact on completed activities and data.
- d. Describes processes for archiving and retrieving configuration items.

3.3.3 Manage Development Errors

Ref	Principle	Applicability
4	The development assurance process ensures that discovered development errors are managed.	All failure condition classifications

A development assurance process that meets this principle:

- a. Defines a process to identify and record development errors.
- b. Defines a process to disposition development errors, by either resolving these errors or evaluating to determine that the impacts of these errors are acceptable at all applicable levels. Resolving the development errors includes reducing the likelihood of these errors reoccurring, when appropriate.

3.3.4 Manage Assumptions

Ref	Principle	Applicability
5	The development assurance process ensures that assumptions made during the product development process are managed throughout the lifecycle.	All failure condition classifications

A development assurance process that meets this principle:

- a. Defines a process to identify and record assumptions during the development process.
- b. Defines a process to disposition assumptions during the development process, including recording decisions and rationale.
- c. Ensures that assumptions are reassessed when design or production modifications are made throughout the lifecycle of the product.

3.4 Define the Product

3.4.1 Identify Product Functions

Ref	Principle	Applicability
6	The development assurance process ensures that the product's intended functions are identified and recorded.	All failure condition classifications

A development assurance process that meets this principle:

- a. Identifies the product's intended functions.
- b. Confirms the complete and correct definition of the product's intended functions.
- c. Ensures that the results of these activities are recorded.

3.4.2 Define and Validate Requirements

Ref	Principle	Applicability
7	The development assurance process ensures that a complete, correct, and detailed understanding of the product and its constraints is identified and recorded.	Minor and above

A development assurance process that meets this principle:

- a. Defines the product's functional performance, interface, and other requirements, including:
 1. Requirements are defined with respect to the product's constraints, including operating environment, operating limitations, installation limitations, maintenance constraints, and human/machine interactions.
 2. Product performance is defined. Quantitative performance metrics, which provide measurable, precise, and consistent objectives, are recommended over qualitative performance measures.
 3. Functionality and other characteristics of the product that emerge based on architecture decisions are captured in requirements.
- b. When multiple layers of requirements are defined, relationships between requirements in the layers are established.
- c. Confirms the completeness and correctness (e.g., unambiguity, accuracy, consistency, and verifiability) of the individual requirements and collective requirement sets, identifying omissions and errors, so that the product will meet its intended functions while mitigating or eliminating unintended behaviors.
- d. Ensures that the results of these activities are recorded.

3.4.3 Identify Functional Safety Effects

Ref	Principle	Applicability
8	The development assurance process ensures the functional safety effects that result from failures are identified, evaluated, and recorded.	All failure condition classifications

A development assurance process that meets this principle:

- a. For each function, identifies the set of failure conditions associated with malfunction or loss of function.
- b. For each failure condition, describes the applicable circumstances, which may include phase of flight, operating environment, operator recognition, and external influences.
- c. Describes the effects of each failure condition, including expected or required operator interventions.
- d. Determines and substantiates the failure condition classifications based on the severity of the effects.
- e. Ensures that the results of these activities are recorded.

3.4.4 Analyze Proposed Architecture

Ref	Principle	Applicability
9	The development assurance process ensures that the proposed product architecture is aligned with the safety objectives.	Applicability identified with each item

A development assurance process that meets this principle:

- a. (Applicable to all failure condition classifications.) Identifies a proposed architecture aligned to functional need, including logical elements, and interconnections, as well as structural and spatial relationships.
- b. (Applicable to major and above.) Ensures that safety objectives are established for each failure condition based on its classification. Ensures a logical and acceptable inverse relationship between the likelihood and consequence of each failure condition.
- c. (Applicable to major and above.) Ensures that architectural mitigation strategies to eliminate or reduce the likelihood of the failure conditions in the proposed product architecture are identified.
- d. (Applicable to major and above.) Confirms that the proposed architecture satisfies the safety objectives associated with the product's failure conditions. Also, ensures that the architecture is modified if it does not satisfy the safety objectives.
- e. (Applicable to all failure condition classifications.) Ensures that hazards inherent in the product, are identified.
- f. (Applicable to major and above.) Confirms that the proposed architecture includes appropriate mitigation strategies to address those hazards inherent in the implementation of the product. Also, ensures that the architecture is modified if it does not address the hazards.
- g. (Applicable to hazardous and above.) Confirms that the proposed architecture includes appropriate mitigation strategies to address common causes. Also, ensures that the architecture is modified if it does not address the common causes.
- h. (Applicable to all failure condition classifications.) Ensures that the results of these assessments are recorded.

3.5 Evaluate the Implementation

3.5.1 Verify Implementation

Ref	Principle	Applicability
10	The development assurance process ensures the product performs its intended functions within the product's constraints.	Minor and above

A development assurance process that meets this principle:

- Defines a process to verify that the implementation meets its corresponding requirements.
- Demonstrates that the implementation correctly performs its defined functions throughout the operating environment. Ensures the implementation is reassessed and modified if it does not perform its defined functions.
- Ensures that the results of these evaluations are recorded.

3.5.2 Assess Unintended Behaviors

Ref	Principle	Applicability
11	The development assurance process ensures the implemented product is evaluated for unintended behaviors and that any identified are acceptable.	Major and above

A development assurance process that meets this principle:

- Ensures the implementation is assessed for unintended behavior, including cascading failure effects, to minimize the likelihood of unforeseen hazards. The unintended behaviors evaluation identifies and assesses expected and unexpected effects and confirms operator or maintainer responses. Methodology for evaluating the unintended behaviors may include analyzing or intentionally inducing abnormal inputs, conditions, or performance characteristics.
- Ensures the design is reassessed and revised if unintended behaviors are found. An unintended behavior is a development error which is addressed in [3.3.3](#).
- Ensures that the results of these evaluations are recorded.

3.5.3 Evaluate Implementation

Ref	Principle	Applicability
12	The development assurance process ensures that the implemented product is aligned with the safety objectives.	Applicability identified with each item

A development assurance process that meets this principle:

- (Applicable to major and above.) Confirms that the implementation satisfies the safety objectives associated with the product's failure conditions. Also, ensures that the design is modified if it does not satisfy the safety objectives.
- (Applicable to all failure condition classifications.) Confirms that the implementation includes appropriate mitigation strategies to address those hazards inherent in the implementation of the product. Also, ensures that the design is modified if it does not effectively address the hazards.
- (Applicable to hazardous and above.) Confirms that the implementation includes appropriate mitigation strategies to address common causes. Also, ensures that the design is modified if it does not address the common causes.
- (Applicable to all failure condition classifications.) Ensures that the results of these assessments are recorded.

4. NOTES

4.1 Revision Indicator

A change bar (I) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document, including technical revisions. Change bars and (R) are not used in original publications, nor in documents that contain editorial changes only.

PREPARED BY SAE S-18 AIRCRAFT AND SYS DEV AND SAFETY ASSESSMENT COMMITTEE